

Kaseya
365
USER

**SUBSCRIPTION
COMPONENTS**

TABLE OF CONTENTS



PREVENT

USER AWARENESS TRAINING + TESTING – BullPhish ID

ANTI-PHISHING DEFENSE – Graphus

DARK WEB MONITORING – Dark Web ID

RESPOND

CLOUD DETECTION + RESPONSE – SaaS Alerts

RECOVER

SAAS BACKUP – Spanning

OR

SAAS BACKUP – Backupify

Kaseya
365
USER

PREVENT

Make Your Employees Your Biggest Cybersecurity Asset

The No. 1 cause of cybersecurity incidents at any organization is the same: human error. Every day, employees are bombarded with email messages and any staff member—from intern to CEO—could be the target of a phishing attack that results in a costly cybersecurity incident. The attacks are growing more and more sophisticated, and even the most effective email security tools are not 100% foolproof. This makes employees an important layer of defense between cybercrime and your organization.

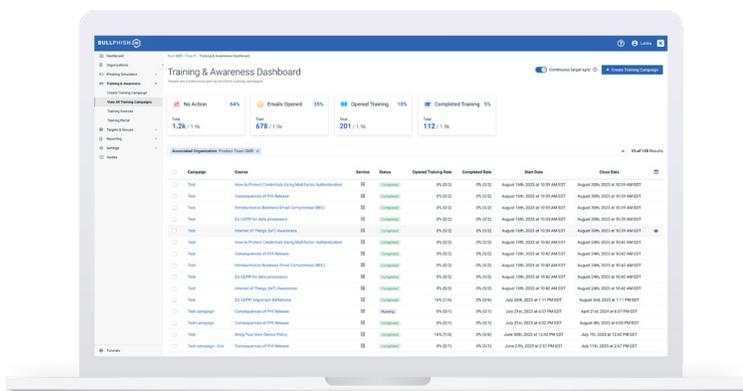
SECURITY AWARENESS AND ANTI-PHISHING TRAINING EDUCATES AND EMPOWERS YOUR EMPLOYEES AND HELPS SECURE YOUR ORGANIZATION.

The importance of conducting regular, ongoing security awareness training that keeps up with the latest threats cannot be overstated. The goal is to have savvy, vigilant employees who recognize and avoid potential security threats and practice safe online behavior.

Having well-trained staff—whether they work in the office, on the road or from home—enhances your company’s cybersecurity posture, fulfills compliance and cyber insurance requirements and reduces the likelihood of a devastating cyberattack.



SECURITY AWARENESS TRAINING REDUCES YOUR RISK OF EXPERIENCING A CYBERATTACK BY UP TO 70%



BULLPHISH ID MAKES TRAINING EASY

- Set-it-and-forget-it campaign management
- Integration with Microsoft 365 and Google Workspace for seamless group and user management
- Short, engaging training videos in 8 languages
- Phishing simulations that reflect common threats
- Options for plug-and-play and customizable phishing kits
- BONUS: Upload your own training content and use our platform to deliver it

EFFORTLESS SECURITY AWARENESS TRAINING

Your employees are your first and primary line of defense against cyberattacks and online fraud. BullPhish ID helps you equip them with the knowledge and skills they need to protect both themselves and your organization from costly cyberattacks.



SIMULATED PHISHING ATTACKS | SECURITY AWARENESS TRAINING



EASY CAMPAIGN MANAGEMENT

Easily manage employee groups for phishing and training campaigns via continuous Active Directory sync. Run different campaigns for multiple groups and schedule campaigns to be sent out at random times to prevent employees from warning each other. Schedule campaigns ahead of time and they'll run automatically at the designated times.



CUSTOMIZABLE TO YOUR NEEDS

Customize your phishing exercises to suit the distinct needs of your organization and specific employee groups, tailoring emails to the threat types they are likely to encounter. Use our pre-loaded email templates or create your own emails from a blank template. Increase your training campaign effectiveness by customizing sending domains to appear as if the emails come from your own domain.



ENGAGING TRAINING

Our short and visually engaging training videos deliver easy-to-digest material and are offered in English, French, German, Italian, Dutch, Portuguese (Brazil), Spanish (Iberian/European) and Spanish (Latin American). Each lesson is coupled with an online quiz to test the employees' understanding of the training content.



ALWAYS ON TOP OF THREAT TRENDS

With ever-evolving cyberthreats, it's important that your employees are exposed to the latest traps set by criminals. We regularly update our phishing kits and training courses to cover the most up-to-date phishing scams, so your employees are ready when real threats arrive.



MEASURE AND TRACK

Our reporting is automated and includes employee phishing exercise and training campaign results, helping you assess your organization's cybersecurity posture and identify employees who exhibit risky online behavior and need additional training.



SATISFY COMPLIANCE AND CYBER INSURANCE REQUIREMENTS

Having strong security protections in place, including an employee security awareness training program, is now a requirement to qualify for or to renew a cyber insurance policy. You also may be subject to various government regulations, with new cybersecurity, data-handling and privacy laws coming out all the time. Stay on top of your compliance requirements with our robust selection of compliance training courses that include HIPAA, GDPR, PCI-DSS, CMMC, NIST 800-171 and more.

BULLPHISH ID



Simple, Powerful, Automated!

Anti-phishing Defense for Microsoft 365 & Google Workspace

Graphus is a simple, powerful and cost-effective automated phishing defense solution for companies of all sizes that protects every employee from email-borne threats – whether they originate outside or inside of your organization.

Graphus enhances your security posture by enabling you to defend employees from email-based cyberattacks including phishing, spear phishing, business email compromise (BEC), account takeover (ATO), identity spoofing, malware and ransomware.

How is Graphus unique?

To uncover these attacks, Graphus employs patented AI technology that monitors communication patterns between people, devices and networks to reveal untrustworthy emails. By focusing on the credibility of each interaction, Graphus identifies and blocks social engineering attacks targeting employees to keep your organization safe from today's biggest threats.

Why add Graphus to your organization's security stack?

Make your organization more secure:

- Get comprehensive email security with 3 layers of defense
- Prevent costly security incidents and improve your cyber resilience
- Keep your business compliant with regulatory and cyber insurance requirements

Make your IT team more efficient:

- Graphus is API-based with no email re-routing or agents to install
- Deploy across the enterprise within minutes
- Streamline security operations through workflow automation

Make your IT operations more cost-effective:

- Pay only for what you need (per-inbox pricing)
- Avoid financial and reputation damage from security incidents
- Integrate real-time intel into your existing threat intelligence programs



3 Layers of Defense for Microsoft 365 and Google Workspace Inboxes

1. TrustGraph automatically detects and quarantines malicious emails that slip through your organization’s cloud email security or existing secure email gateway (SEG), preventing employees from interacting with harmful messages.

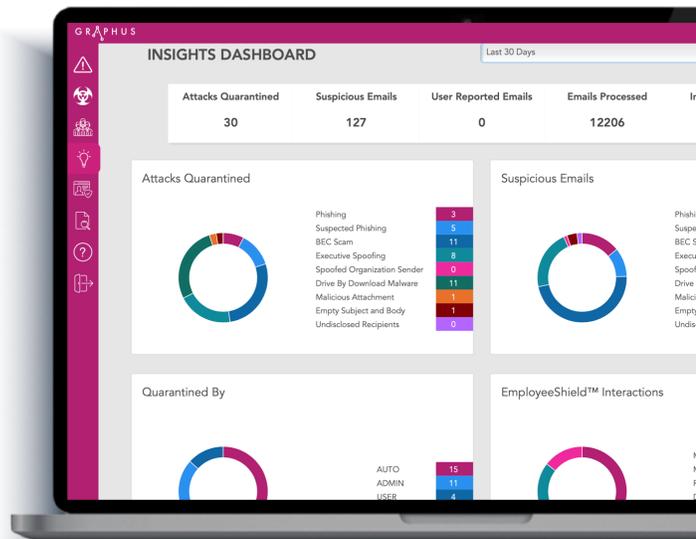
2. EmployeeShield places an interactive warning banner at the top of suspicious messages to alert the email recipients and allow them to report a message as phishing, block it as junk or mark it as safe with one click.

3. Phish911 empowers employees to bolster email security by proactively quarantining messages they deem suspicious for IT to investigate.

Personal Graymail Filter gives employees the ability to mark a message as spam with one click to stop receiving email from that sender – building a personal spam profile for each individual email recipient. The filter blocks the sender for that individual user only, so other employees who may want to continue receiving email from that sender won’t be affected.

The intuitive and robust Graphus Insights Dashboard allows your IT team to monitor your real-time security posture, enabling you to quickly investigate and take action on detected threats.

The reporting feature of the dashboard generates informative security metrics reports you can use in security briefings with the leadership.



GRAPHUS	VS	Secure Email Gateways
ACTIVATION TAKES MINUTES 3-click activation in Microsoft 365. Start protecting your organization instantly. No email configuration required.		ACTIVATION TAKES WEEKS An organization is left unprotected during the weeks or even months it takes to deploy an SEG.
NO DELAY IN RECEIVING EMAILS Analyzes messages in real time with no delay in email delivery. Safe messages are never quarantined.		DELAYS EMAILS SEG filtering can cause delays in receiving messages or improper quarantine of safe emails.
DETECTS ZERO-DAY ATTACKS Powered by patented AI technology, the TrustGraph algorithm detects zero-day attacks in real time.		ZERO-DAY ATTACKS SLIP BY SEGs use traditional threat intelligence to detect attacks, allowing zero-day attacks to slip into inboxes.
AUTOMATED PHISHING DEFENSE Integrates at the API level to detect and stop sophisticated social engineering attacks.		LIMITED PHISHING DETECTION Built to stop spam and malicious emails, not sophisticated social engineering attacks.
EMPLOYEEESHIELD™ VISUAL NOTIFICATION Provides an interactive warning banner to alert your employees to suspicious emails and give them a simple way to report threats.		EMPLOYEES AREN'T NOTIFIED Employees are not warned of suspicious messages, leaving organizations extremely vulnerable to an attack.

Actionable Threat Intel for Your Organization

With cyberthreats increasing every day, Dark Web ID helps ensure you are proactively protecting your company's brand, employees and executives.

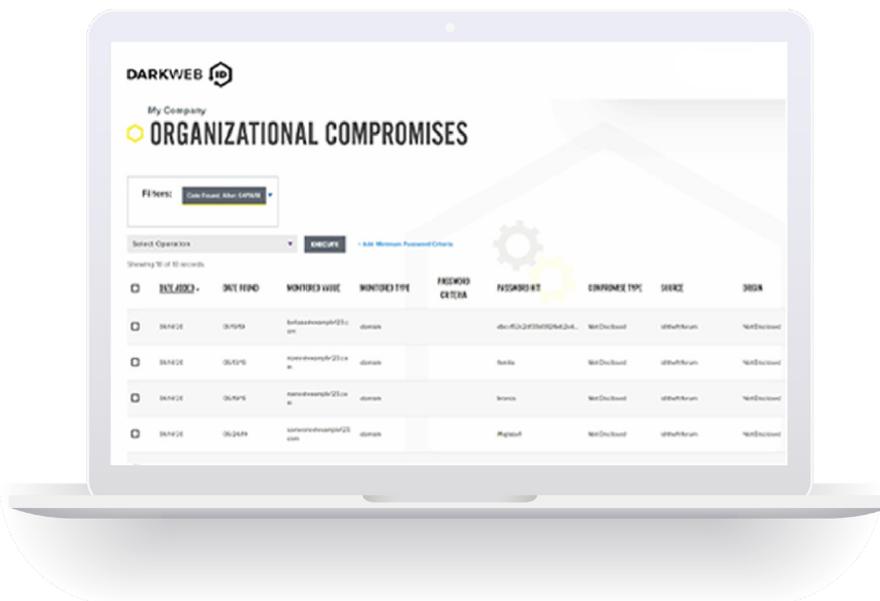
Gain deeper awareness into your security gaps—before cybercriminals get the chance to exploit them and steal from you.

Stolen user credentials (email addresses and passwords) found on the dark web can indicate that your company or a third-party application or website used by your employees has been compromised—so you can take immediate action.

Cybercriminals traffic and buy stolen credentials so they can infiltrate your networks to steal your data. By monitoring the dark web for threat intelligence about stolen user data associated with your company's domains, you can be alerted when a compromise is detected and then respond to stop a potentially costly and devastating data breach.

60%

of the information available on the dark web could potentially harm enterprises



MONITOR 24/7/365

- Hidden chat rooms
- Unindexed sites
- Private websites
- Peer-to-peer (P2P) networks
- IRC (internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

MONITOR, IDENTIFY AND MITIGATE THREATS



Your business security strategy extends far beyond your network, and Dark Web ID can help strengthen it. Easily monitor for exposure and leverage rich threat intelligence to take the appropriate actions that will protect your company's assets and reputation and lower the risk of breach.

SAAS BUSINESS APPLICATIONS INCREASE RISK

Although web-based applications allow employees to do their jobs from most anywhere, they also open up your organization to risk. Payroll and HR platforms, CRM and marketing automation tools, travel sites, banking sites and social media accounts are accessed by your employees many times throughout a day. A recent survey shows that 65% of people reuse the same password for multiple or all accounts—potentially the same one they use to log in to your network.

EMAIL MONITORING FOR HIGHLY TARGETED EXECS AND PRIVILEGED USERS

Your executives and administrative users often have greater access to systems, information and sensitive data. If their personal email credentials are compromised and they happen to reuse the same credentials at work, the attackers may use them to gain access to corporate systems. The attackers may also use social engineering to impersonate your executives to trick other employees to give up access, divert funds, or for other schemes. Therefore, it's important to monitor the personal mail addresses of your executive and administrative users along with their corporate email accounts.

EXTEND SECURITY TO THE SUPPLY CHAIN

Some cyberattacks could happen due to exposure to third-party vendors from your supply chain. The interwoven systems of vendors and partners present security risks since data is shared across networks. The growing need for cyber supply chain risk management has prompted forward-thinking organizations to add dark web monitoring to vendor due diligence.

QUICKLY PROVIDE YOUR IT SECURITY TEAM THREAT INTELLIGENCE

Are your security teams resource-constrained and focused on detecting and mitigating threats rather than installing new technology for monitoring? Dark Web ID takes just minutes to set up and will start showing compromise results right away. Reporting is flexible and can be integrated with your Security Operations Center (SOC) and other alerting and remediation platforms with available APIs.

HOLISTIC VISIBILITY

By adding Dark Web ID monitoring to your security strategy, you will get a more complete picture of your company's security posture. Not only does it serve as an early warning mechanism that alerts you before breaches occur, it also provides invaluable data analytics to evaluate where employees need security awareness training or where multi-factor authentication and single sign-on are warranted.

Kaseya
365
USER

RESPOND

SaaS Alerts®

Automatically Detect and Remediate Security Breaches in SaaS Applications

Imagine having a watchful protector that never sleeps, constantly guarding your employees SaaS applications. Our platform does just that, detecting unauthorized access, and shutting it down without breaking a sweat.



The Most Comprehensive SaaS Security Platform Available



**MONITORING
& ALERTING**



**24/7 DETECTION &
RESPONSE**



**SECURITY
CONFIGURATIONS**



**MONITOR MORE
APPLICATIONS**



**RMM &
IT DOCUMENTATION
TOOL MONITORING**



**EXECUTIVE
REPORTS**

How Does SaaS Alerts differ from MDR providers?

MDR providers rely on human “threat hunters” which are tasked with aggregating data from multiple sources and responding as quickly as possible, usually measuring response time in hours. SaaS Alerts provides alerting and remediation steps with actions taken within seconds of malicious activity **with no human interaction required**. This difference significantly minimizes the risk of data egress or malicious activity within your most vulnerable environments.

A Deeper Look into SaaS Alerts

MONITORING AND ALERTING

We use machine learning to aggregate and analyze user behavior in SaaS platforms. When unusual behavior is detected, you get an instant notification so you can take action fast.

24/7 DETECTION AND RESPONSE

SaaS Alerts automatically responds to detected threats and account compromises, temporarily disabling the account and blocking new login attempts. Automated threat mitigation occurs within minutes of detection and provides detailed forensic logs of compromised data and remediation steps.

SECURITY CONFIGURATIONS

Microsoft security recommendations are complex and require a lot of time to implement. With SaaS Alerts, you can apply security recommendations across your entire environment in minutes and receive alerts if a security score regresses.

BEYOND MICROSOFT 365

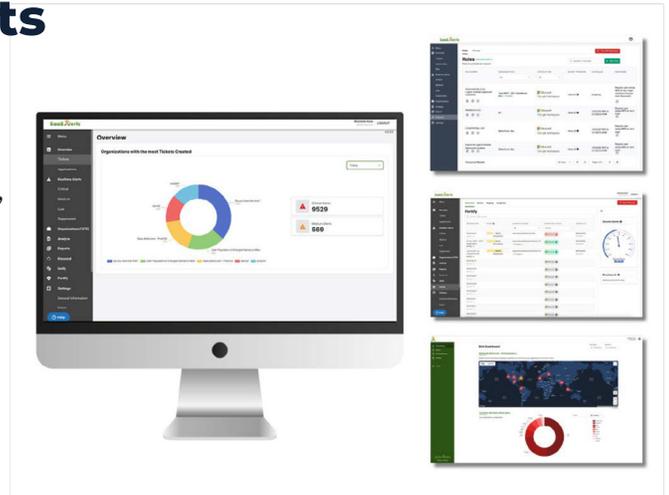
With our App Wizard, we can quickly integrate with any SaaS application with a viable API to pull mission-critical data into SaaS Alerts, so you can quickly detect and respond to SaaS security threats across almost all of your SaaS applications.

USER IDENTITY VALIDATION

Reconcile device data with SaaS data to ensure only authorized users on authorized devices can gain access to critical company SaaS applications.

INTUITIVE REPORTING

Powerful reporting of user behavior and SaaS application events provides a comprehensive and timely view of the current state of SaaS security for your executives and stakeholders.



CORE APPLICATIONS WE PROTECT



SaaS Alerts®

Kaseya
365
USER

RECOVER



Backup Purpose-Built for Microsoft 365 and Google Workspace

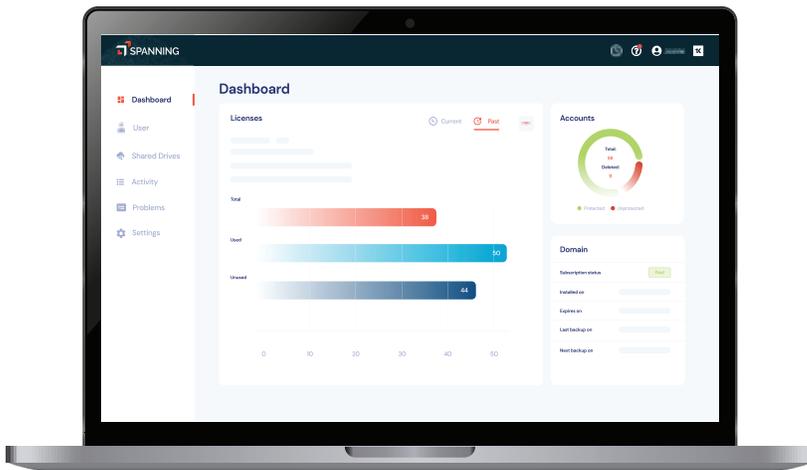
You’ve made the move to the cloud to save time, simplify collaboration, and free up valuable resources, but now it’s up to you to protect that data. Under the shared responsibility model, Microsoft and Google guarantee application availability, but you’re responsible for protecting data against ransomware, user errors, and other internal and external threats.

But you can eliminate the fear and uncertainty of data loss with Spanning – a complete, reliable backup solution for Microsoft 365 and Google Workspace. Spanning combines robust data protection, powerful backup automation, versatile recovery options, and multi-layered data security for true peace of mind.

24000+
BUSINESSES DEFENDED

2.5 MILLION USERS
USERS PROTECTED

3.9 BILLION
BACKUPS PER WEEK



Spanning was designed to streamline the backup and recovery process. The platform provides powerful, yet easy-to-use capabilities for both administrators and end-users.

Accomplishing backup and restore of Microsoft 365 and Google Workspace data has never been so simple and intuitive.

SIMPLIFY AND STREAMLINE BACKUP PROCEDURES

Say goodbye to backup headaches; daily, automated SaaS backups and unlimited on-demand backups ease the burden and provide you with as many backup points as necessary.

RECOVER WHAT YOU NEED, WHEN YOU NEED IT

Powerful functionalities like granular search-based restore, point-in-time restore, and self-restore for end users allow you to recover effectively in a matter of minutes.

KEEP YOUR SAAS DATA SECURE AND COMPLIANT

Layered security, top-tier data protection practices, and extensive certifications with third-party regulations provide reassurance that your data is safe and up to code.

SIMPLY SMARTER BACKUP & RECOVERY



DAILY, AUTOMATED BACKUP

Spanning automatically completes daily backups as part of a recurring, incremental backup process. Each and every day, this auto-discovery and backup of new and/or altered content runs quietly in the background with zero additional effort from your admins or users. **Simply “set it and forget it.”**

CUSTOMIZABLE, ON-DEMAND BACKUP

If daily, automated backups don't provide you with enough backup points for comfort, you can supplement with on-demand backups as often as you like. These backups can be customized to your needs and are unlimited, allowing you to create as many backup points as necessary.

GRANULAR, SEARCH-BASED RESTORE

Simply search, and once you've find the data you're looking for, you can choose to restore individual items, multiple items, or entire folders. Granular restore options afford you maximum control.

END USER SELF-SERVICE RESTORE

Minimize the burden on admins by empowering your end users with Spanning's self-service restoration capabilities. Licensed users may be permitted to restore their own files, folders, and content. With zero IT intervention, restores can be accomplished quickly to ensure maximum productivity.

ROBUST ADMIN FUNCTIONALITY

Manage backups effectively with admin capabilities such as cross-user restore. Admins are able to restore data back into original user accounts, or into a different user's account altogether. Admins can also customize backup settings and distribute licenses to align with organizational needs.

ON-THE-GO, MOBILE ACCESS

Spanning was designed to accommodate the mobile-first, cloud-first mentality and on-the-go nature of today's workforce. The mobile-friendly user interface enables accurate restore of Microsoft 365 data anytime, anywhere. All you need is a Microsoft supported desktop, tablet, or mobile device.

MULTI-LAYERED SECURITY

HIGH AVAILABILITY

99.9% uptime SLA
(service level agreement)

DATA ENCRYPTION

128-bit SSL in transit
and 256-bit AES at rest

GLOBAL DATA CENTERS

AWS data centers located in
the U.S., Canada, EU, UK,
and APAC regions

ACCESS CONTROL

Production server access is
granted only to named Spanning
employees who have specific
operational requirements

INTRUSION DETECTION

Active guard with log analysis file
integrity checking, policy monitoring
rootkit detection, real-time altering
and active response

CREDENTIAL PROTECTION

Optional dark web monitoring
alerts of compromised accounts
and credentials

COMPLIANCE CERTIFICATIONS

HIPAA, GDPR, ISO 27001, SOC 2 Type II
ISSAE 16 & ISAE 3402), SAS-70 Type II,
US-EU Privacy Shield, BBB EU Privacy
Shield, and Swiss-US Privacy Shield





Backupify for Microsoft 365 and Google Workspace

You've made the move to the cloud to save time, simplify collaboration, and free up valuable resources, but now it's up to you to protect that data. Under the shared responsibility model, Microsoft and Google guarantee application availability, but you're responsible for protecting data against ransomware, user errors and other internal and external threats.

But you can eliminate the fear and uncertainty of data loss with Backupify – a complete, reliable backup solution for Microsoft 365 and Google Workspace. Backupify combines robust data protection, powerful backup automation, versatile recovery options, and multi-layered data security for true peace of mind.



**SIMPLIFY AND STREAMLINE
BACKUP PROCEDURES**



**RECOVER WHAT YOU NEED,
WHEN YOU NEED IT**



**KEEP YOUR SAAS DATA SECURE
AND COMPLIANT**

Backupify was designed to streamline the backup and recovery process. The platform provides powerful, yet easy-to-use capabilities. Accomplishing backup and restore of Microsoft 365 and Google Workspace data has never been so simple and intuitive.



Secure Office 365 data protection. Backupify delivers fast recovery of Exchange, OneDrive, SharePoint Online, Calendar, Contacts and Microsoft Teams data.



Google Vault alone does not ensure your G Suite data is recoverable. Quickly restore lost data from Gmail, Calendars & Contacts, Drive and Shared Drives with Backupify.

The SaaS Backup Solution MSPs Love

AUTOMATED, CONTINUOUS SAAS BACKUPS

Protect Microsoft 365 and Google Workspace applications against accidental or malicious deletion, ransomware attacks, and other cloud data loss with up to 3x daily, automated backups.

RECOVER QUICKLY

Easily avoid business downtime with quick a one-click restore process. Quickly identify and recover individual items or entire folders without overwriting existing files.

COMPLETE CONTROL

Have complete administrative control and proactively monitor your backup activities. Be confident in the status of all backup and recovery operations with our detailed, actionable dashboard.

BEYOND FILES AND FOLDERS

A true SaaS backup solution protects not just files and folders, but collaboration tools like Microsoft Teams, SharePoint, OneDrive, and Google Drive.



backupify

backupify

Kaseya 365 USER

SUBSCRIPTION COMPONENTS

Go beyond the keyboard to protect the critical data and identity of all the users you manage in a single Kaseya 365 User subscription.

[EXPLORE KASEYA 365 USER](#)